



9110-04

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0056]

Privacy Act of 1974; Department of Homeland Security/United States Coast Guard – 029

Notice of Arrival and Departure System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security (DHS) system of records titled, “Department of Homeland Security/United States Coast Guard - 029 Notice of Arrival and Departure System of Records.” This system of records allows the Department of Homeland Security/United States Coast Guard (USCG) to facilitate the effective and efficient entry and departure of vessels into and from the United States, and assist with assigning priorities for conducting maritime safety and security regulations. As a result of a biennial review of this system, the Department of Homeland Security/United States Coast Guard is updating this system of records notice to update the system manager and address category. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security’s inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0056 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Marilyn Scott-Perez, (202) 475-3515), Privacy Officer, Commandant (CG-61), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) United States Coast Guard (USCG) proposes to update and reissue a current DHS system of records titled, “DHS/USCG - 029 Notice of Arrival and Departure System of Records.” The collection and maintenance of this information will assist DHS/USCG in meeting its statutory obligation to assign priorities while conducting maritime safety and security missions in accordance with international and U.S. regulations. As a result of a biennial review of the system, the system manager and address category has been updated to reflect the new mail stop.

Consistent with DHS’s information sharing mission, information stored in the DHS/USCG - 029 Notice of Arrival and Departure (NOAD) may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USCG may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This updated system will be included in DHS’s inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals’ records. The Privacy Act applies to information that is maintained in a “system of records.” A “system of records” is a group of any records

under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCG-029 Notice of Arrival and Departure System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/USCG-029

System name:

DHS/USCG-029 Notice of Arrival and Departure System of Records

Security classification:

Unclassified

System location:

Records are maintained at the United States Coast Guard (USCG) Operations Systems Center, Kearneysville, West Virginia (WV), and other field locations. Ship Arrival Notice is the information technology (IT) system in which records associated with this function are maintained.

Categories of individuals covered by the system:

Categories of individuals covered by this notice consist of crew members who arrive and depart the U.S. by sea and individuals associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure, including but not limited to vessel owners, operators, charterers, reporting parties, 24-hour contacts, company security officers, and persons in addition to crew who arrive and depart the U.S. by sea.

Categories of records in the system:

- Records on vessels includes: name of vessel; name of registered owner; country of registry; call sign; International Maritime Organization (IMO) number or, if a vessel does not have an IMO number the official number; name of the operator; name of charterer; and name of classification society.
- Records on arrival information pertaining to the vessel includes: names of last five foreign ports or places visited by the vessel; dates of arrival and departure for last five foreign ports or places visited; for each port or place of the U.S. to be visited, the name of the receiving facility; for the port or place of the U.S., the estimated date and time of arrival; for the port or place in the U.S., the estimated date and time of departure; the location (port or place and country) or position (latitude and longitude or waterway and mile marker) of the vessel at the time of reporting; and the name and telephone number of a 24-hour point of contact (POC).

- Records on departure information as it pertains to the voyage includes: the name of departing port or waterways of the U.S.; the estimated date and time of departure; next port or place of call (including foreign); the estimated date and time of arrival; and the name and telephone number of a 24-hour POC.
- Records on crewmembers include: full name; date of birth; nationality; identification type (for example, passport, U.S. Alien Registration Card, U.S. Merchant Mariner Document, foreign mariner document, government issued picture Identification (ID) (Canada), or government-issued picture ID (U.S.), number, issuing country, issue date, expiration date); position or duties on the vessel; where the crewmember embarked (list port or place and country); and where the crewmember will disembark.
- Records for each individual onboard in addition to crew include: full name; date of birth; nationality; identification type (for example: passport, U.S. alien registration card, government-issued picture ID (Canada), government-issued picture ID (U.S.), number, issuing country, issue date, expiration date); U.S. address information; and from where the person embarked (list port or place and country).
- Records related to cargo onboard the vessel include: a general description of cargo other than Certain Dangerous Cargo (CDC) onboard the vessel (e.g., grain, container, oil); name of each CDC carried, including United Nations (UN) number, if applicable; and amount of each CDC carried.

- Records regarding the operational condition of equipment required by 33 Code of Federal Regulations (CFR) part 164; the date of issuance for the company's document of compliance certificate; the date of issuance of the vessel's safety management certificate; and the name of the flag administration, or recognized organization(s) representing the vessel flag administration that issued those certificates.

Authority for maintenance of the system:

Departmental Regulations, 5 U.S.C. 301; 14 U.S.C. 632; 33 U.S.C. 1223; 46 U.S.C. 3717; 46 U.S.C. 12501; Federal Records Act of 1950, Public Law 90-620; the Maritime Transportation Act of 2002, Public Law 107-295; the Homeland Security Act of 2002, Public Law 107-296; 33 CFR part 160; and 36 CFR chapter XII.

Purpose(s):

The purpose of this system is to maintain NOAD information to screen individuals and cargo associated with vessels entering or departing U.S. waterways for maritime safety, maritime security, maritime law enforcement, marine environmental protection, and other related purposes.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
4. The U.S. or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To federal and foreign government intelligence or counterterrorism agencies or components if USCG becomes aware of an indication of a threat or potential threat to national or international security, or if such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

I. To an organization or individual in either the public or private sector, foreign or domestic, if there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life, property, or other vital interests of a data subject and disclosure is proper and consistent with the official duties of the person making the disclosure;

J. To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, appropriate notice will be provided of any identified health threat or risk to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantined disease or for combating other significant public health threats;

K. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, settlement negotiations, response to a subpoena, or in connection with criminal law proceedings;

L. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure

is appropriate in the proper performance of the official duties of the officer making the disclosure;

M. To an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request;

N. To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations if USCG is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.

O. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

USCG stores NOAD information electronically in the Ship Arrival Notice System (SANS) located at USCG Operations Systems Center in Kearneysville, WV. USCG uses an alternative storage facility for the SANS historical logs and system backups.

Derivative NOAD system data may be stored on USCG Standard Workstation III computers or USCG unit servers located at USCG Headquarters, headquarters units, area offices, sector offices, sector sub-unit offices, and other locations where USCG authorized personnel may be posted to facilitate DHS' mission.

Retrievability:

USCG retrieves records from the SANS by vessel and then extracted by name, passport number, or other unique personal identifier. NOAD information maintained in the SANS is not directly retrievable by name or other unique personal identifier.

Safeguards:

USCG safeguards NOAD data in the SANS in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. USCG file areas

are locked after normal duty hours and the facilities are protected from the outside by security personnel. The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified and Accredited in accordance with the requirements of the Federal Information Security Management Act (FISMA).

Retention and disposal:

In accordance with NARA Disposition Authority number N1-026-05-11, NOAD information on vessels and individuals maintained in the SANS is destroyed or deleted when no longer needed for reference, or after ten years, whichever is later. Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties, for example, Captain of the Port and marine safety offices, sea marshals, Customs and Border Patrol, Immigration and Customs Enforcement with the necessary information to set up security zones, scheduling boarding and inspections activities, actions for non-compliance with regulations, and other activities in support of USCG's mission to provide for safety and security of U.S. ports, are deleted after five years if they do not constitute a permanent record according to NARA.

System Manager and address:

Commandant (CG-26), United States Coast Guard, Mail Stop 7301, Washington, D.C. 20593-0001.

Notification procedure:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and USCG's Freedom of Information Act (FOIA) Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, D.C. 20528-0655.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See “Notification procedure” above.

Contesting record procedures:

See “Notification procedure” above.

Record source categories:

USCG obtains NOAD records from vessel carriers and operators regarding passengers, crewmembers, and cargo that arrive in, depart from, or transit through the U.S. on a vessel carrier covered by notice of arrival and departure regulations.

Exemptions claimed for the system:

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated.

Dated: October 23, 2014.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2014-25905 Filed 10/30/2014 at 8:45 am; Publication Date: 10/31/2014]